EXHIBIT
A

Web | Moving Images | Texts | Audio | Software | Education | Patron Info | About IA

Forums | FAQs | Contributions | Jobs | Donate

Search:

All Media Types GO!

Anonymous User (login or join us)

Announcements
(more)

Bookmark explorer

Dead update

Katrina web archive launches, over 25 million pages, text searchable

Web

55 billion pages

WaybackMachine

http://www.csl.sri.com

Take Me Back | Advanced Search

Welcome to the Archive RSS

The Internet Archive is building a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, and the general public.

Moving Images

38,529 movies

Browse (by keyword)
Upload your own movie

This Just In (more) RSS

9-11 Conspiracy Video -...
1 hour ago

Curator's Choice (more)

Youth Media Clip
Vicki Chan, senior at Skyline High school, shows

Live Music Archive

37,280 concerts

Browse (by band)
Upload your own concert

This Just In (more) RSS

Derek Trucks Band Live...
44 minutes ago

Curator's Choice (more)

Live Music Archive

Ari Hest Live at Willard Straight Hall Memorial...
1. Intro 2. Fond Farewell 3. Caught Up In Your Love 4. Sleep Tonight 5. The Upper Hand 6. When If...

Audio

87,957 recordings

Browse (by keyword)
Upload your own recording

This Just In (more) RSS

Crap From The Past -...
24 minutes ago

Curator's Choice (more)

Texts

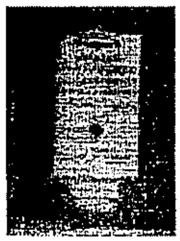
30,351 texts

Browse (by keyword)
Upload your own text

This Just In (more) RSS

Mes 10 ans
26 minutes ago

Curator's Choice (more)



us how two Oakland Public School teachers transfer....

Starfrosch - Top of the pods - Plainaudio session...
___ PRESCRIPTION In Hamburg wird das Netlabel Plainaudio betrieben. Thomas und Manu heben den....

English embroidered bookbindings

Recent Reviews

Interview Jim Amos
Average rating:

dr_ayman_reta2_amz.rm
Average rating:

Recent Reviews

Grateful Dead Live at Boston Garden on 1993-09-26
Average rating:

Grateful Dead Live at Charlotte Coliseum on 1995-03-23
Average rating:

Recent Reviews

Petit pot de colle
Average rating:

Jon Vaughn, Carrie Gates & Scant Intone - Live At PAVED Arts [pan020]
Average rating:

Recent Reviews

Dont Fool Around
Average rating:

Human Company a sci-fi novel
Average rating:

Most recent posts (write a post by going to a forum) more...

Subject	Poster	Forum	Replies	Views	Date
New THINNER release: Ben Businovski - *Simulacraic Wonderland* [THN088]	LAJ	netlabels	0	3	23 minutes ago
Re: Who do you love?	Yankee9	GratefulDead	0	19	2 hours ago
Re: Who do you love?	midnight sun	GratefulDead	0	24	2 hours ago
Re: 2 part question - Dead Versatility	midnight sun	GratefulDead	1	34	3 hours ago
Re: 2 part question - Dead Versatility	bluedevil	GratefulDead	0	9	3 hours ago
Re: bit torrents	unclejohnnyd	GratefulDead	0	16	3 hours ago
Re: Who do you love?	Rastamon	GratefulDead	0	21	4 hours ago
Re: Who do you love?	bluedevil	GratefulDead	0	13	4 hours ago
Re: Jerry's B-day	Rastamon	GratefulDead	0	33	4 hours ago
Who do you love?	DEADBUCK	GratefulDead	4	104	4 hours ago

Institutional Support

Alexa Internet
HP Computer
The Kahle/Austin Foundation
Prelinger Archives
National Science Foundation
Library of Congress
LizardTech
Sloan Foundation
Hewlett Foundation
Individual contributors

Terms of Use (10 Mar 2001)

Skin: classic | columns | custom!

EXHIBIT
B

INTERNET ARCHIVE WaybackMachine

Enter Web Address: http:// All Take Me Back Adv. Search Compare Archive Pages

Searched for http://www.csl.sri.com

205 Results

Note some duplicates are not shown. See all.
* denotes when site was updated.

Search Results for Jan 01, 1996 - Jul 24, 2006

1996	1997	1998	1999	2000	2001	2002	2003	2004	2005
1 pages	3 pages	3 pages	5 pages	10 pages	27 pages	21 pages	25 pages	33 pages	33 pages
Dec 26, 1996 *	Feb 04, 1997 *	Jan 23, 1998 *	Jan 25, 1999 *	Mar 03, 2000 *	Feb 02, 2001 *	Feb 11, 2002	Jan 27, 2003	Feb 03, 2004	Feb 03, 2005
	Jul 05, 1997	Dec 07, 1998 *	Feb 18, 1999	May 10, 2000 *	Feb 24, 2001	Jun 02, 2002 *	Feb 07, 2003	Feb 08, 2004	Feb 04, 2005
	Dec 11, 1997 *	Dec 12, 1998	Feb 23, 1999	May 11, 2000	Feb 26, 2001	Jun 04, 2002 *	Feb 12, 2003 *	Feb 20, 2004	Feb 05, 2005
			Feb 24, 1999	Jun 22, 2000	Mar 02, 2001	Aug 11, 2002 *	Feb 13, 2003 *	Mar 23, 2004	Feb 06, 2005
			Apr 17, 1999 *	Jul 06, 2000	Mar 07, 2001 *	Sep 26, 2002 *	Mar 21, 2003	Apr 01, 2004	Feb 06, 2005
				Aug 15, 2000	Mar 31, 2001 *	Sep 30, 2002 *	Mar 23, 2003	May 12, 2004	Feb 07, 2005
				Aug 24, 2000 *	Apr 03, 2001	Oct 02, 2002 *	Apr 22, 2003	May 12, 2004 *	Feb 08, 2005
				Oct 18, 2000 *	Apr 04, 2001	Oct 13, 2002 *	Apr 25, 2003 *	May 25, 2004	Feb 11, 2005
				Dec 06, 2000 *	Apr 07, 2001	Oct 15, 2002	May 30, 2003 *	May 27, 2004 *	Feb 12, 2005
				Dec 18, 2000 *	Apr 10, 2001	Oct 19, 2002	Jun 02, 2003	Jun 03, 2004	Feb 14, 2005
					Apr 12, 2001	Oct 25, 2002	Jun 21, 2003 *	Jun 09, 2004	Feb 16, 2005
					Apr 13, 2001	Nov 03, 2002	Jul 23, 2003 *	Jun 10, 2004	Feb 17, 2005
					Apr 14, 2001	Nov 05, 2002	Aug 04, 2003	Jun 11, 2004 *	Feb 20, 2005
					Apr 17, 2001	Nov 11, 2002 *	Aug 05, 2003 *	Jun 12, 2004	Feb 24, 2005
					Apr 18, 2001	Nov 20, 2002	Oct 02, 2003 *	Jun 14, 2004 *	Feb 26, 2005
					Apr 19, 2001	Nov 21, 2002	Oct 10, 2003 *	Jun 16, 2004	Feb 28, 2005
					Apr 23, 2001	Nov 23, 2002 *	Oct 11, 2003 *	Jun 27, 2004	Mar 05, 2005
					Apr 24, 2001	Nov 25, 2002 *	Oct 12, 2003 *	Jul 10, 2004	Mar 06, 2005
					Apr 28, 2001	Dec 01, 2002	Oct 13, 2003 *	Jul 22, 2004	Mar 07, 2005
					Apr 29, 2001	Dec 02, 2002	Nov 19, 2003	Sep 23, 2004 *	Mar 10, 2005
					May 01, 2001	Dec 03, 2002	Nov 20, 2003	Sep 25, 2004 *	Mar 13, 2005
					May 03, 2001		Dec 03, 2003	Oct 12, 2004	Mar 14, 2005
					May 04, 2001		Dec 11, 2003	Oct 13, 2004	Mar 15, 2005
					May 05, 2001		Dec 20, 2003 *	Oct 16, 2004	Mar 16, 2005
					May 08, 2001 *			Oct 19, 2004	

May 16, 2001	Dec 25, 2003 *	Oct 20, 2004	Mar 17, 2005
Dec 01, 2001 *		Oct 24, 2004	Mar 18, 2005
		Oct 29, 2004	Mar 19, 2005
		Oct 31, 2004	Mar 20, 2005
		Nov 15, 2004	Mar 21, 2005
		Nov 25, 2004	Mar 22, 2005
		Nov 29, 2004	Mar 23, 2005
		Nov 30, 2004	Mar 24, 2005
			Mar 26, 2005

Home | Help

Internet Archive | Terms of Use | Privacy Policy

EXHIBIT C

Computer Science Laboratory

SRI International's Computer Science Laboratory (CSL) was founded in 1952, making it one of the first laboratories to focus on computer science. A main CSL objective is to advance the theory and practice in producing complex software and hardware systems that, to a high degree of certainty, have the intended structural and behavioral properties. Another objective is to explore advanced network-based infrastructure for distributed, heterogeneous computing. CSL consists of approximately 30 professionals, plus several graduate students and visiting scientists.

SRI International is one of the world's largest contract research firms. Founded in 1946 in conjunction with Stanford University as the Stanford Research Institute, SRI now employs more than 2600 people and has offices around the world, including laboratories in Australia and the United Kingdom and the David Sarnoff Research Center in Princeton, New Jersey. SRI is located in the San Francisco Bay Area, specifically in Menlo Park, California, near Silicon Valley and Stanford University.

About CSL

- CSL Staff
- Some History Multi-window displays, hypertext, and the mouse were invented at SRI. The first internet message was received here.
- How to get to CSL

Current Research Activities

- Coarse-Grain Parallel Processing
- Database Interoperability
- Formal Methods
- Integrated Circuit Emulation
- Linear Logic and Proof Theory
- Multimedia and Multicast Communications
- Rewriting Logics and Systems
- Secure Systems
- Software Architecture
- Intrusion Detection

Other Activities

- Publications you can browse and download
- Software we make freely available
- Seminars are usually on Mondays at 4pm and are open to all.
- Risks Forum run by Peter Neumann
- Conferences and calls for papers
- Technical Reports - list
- Technical Reports - abstracts

Other Sites

- Other parts of SRI and nearby sites of interest

Computer Science Laboratory, SRI International, 333 Ravenswood Avenue, Menlo Park, California 94025, USA

webmaster@csl.sri.com

SRI International Computer Science Laboratory

SRI International's Computer Science Laboratory (CSL) was founded in 1952, making it one of the first laboratories to focus on computer science. A main CSL objective is to advance the theory and practice in producing complex software and hardware systems that, to a high degree of certainty, have the intended structural and behavioral properties. Another objective is to explore advanced network-based infrastructure for distributed, heterogeneous computing. CSL consists of approximately 30 professionals, plus graduate students and visiting scientists.

SRI International is one of the world's largest contract research firms. Founded in 1946 in conjunction with Stanford University as the Stanford Research Institute, SRI now employs more than 2600 people and has offices around the world, including laboratories in Australia and the United Kingdom and the David Sarnoff Research Center in Princeton, New Jersey. SRI is located in the San Francisco Bay Area, specifically in Menlo Park, California, near Silicon Valley and Stanford University.

About CSL

- CSL Staff
- How to get to CSL
- History
- How to contact CSL

Current Research Activities

- Coarse-Grain Parallel Processing
- Formal Methods
- Linear Logic and Proof Theory
- Rewriting Logics and Systems
- Software Architecture
- Network Engineering and Management
- Database Interoperability
- Integrated Circuit Emulation
- Multimedia and Multicast Communications
- Secure Systems
- Intrusion Detection

Other Activities

- Publications you can browse and download
- Seminars are usually on Mondays at 4pm and are open to all
- Conferences and calls for papers
- Technical Reports - abstracts
- Software we make freely available
- Risks Forum run by Peter Neumann
- Technical Reports - list

Computer Science Laboratory
SRI International
333 Ravenswood Avenue
Menlo Park, California 94025, USA

http://www.csl.sri.com/index.shtml

Last Modified : Thursday, 06-Nov-97 14:16:14 PST

SRI, International Computer Science Laboratory

webmaster@csl.sri.com

SRI International Computer Science Laboratory

SRI International's Computer Science Laboratory (CSL) was founded in 1952, making it one of the first laboratories to focus on computer science. A main CSL objective is to advance the theory and practice in producing complex software and hardware systems that, to a high degree of certainty, have the intended structural and behavioral properties. Another objective is to explore advanced network-based infrastructure for distributed, heterogeneous computing. CSL consists of approximately 30 professionals, plus graduate students and visiting scientists.

SRI International is one of the world's largest contract research firms. Founded in 1946 in conjunction with Stanford University as the Stanford Research Institute, SRI now employs more than 2600 people and has offices around the world, including laboratories in Australia and the United Kingdom and the Sarnoff Corporation in Princeton, New Jersey. SRI is located in the San Francisco Bay Area, specifically in Menlo Park, California, near Silicon Valley and Stanford University.

About CSL

- CSL Staff
- How to get to CSL
- History
- How to contact CSL

Current Research Activities

- Coarse-Grain Parallel Processing
- Formal Methods
- Linear Logic and Proof Theory
- Rewriting Logics and Systems
- Software Architecture
- Network Engineering and Management
- Database Interoperability
- Integrated Circuit Emulation
- Multimedia and Multicast Communications
- Secure Systems
- Intrusion Detection

Other Activities

- Publications you can browse and download
- Seminars are usually on Mondays at 4pm and are open to all
- Conferences and calls for papers
- Technical Reports - abstracts
- Software we make freely available
- Risks Forum run by Peter Neumann
- Technical Reports - list

Computer Science Laboratory
SRI International
333 Ravenswood Avenue
Menlo Park, California 94025, USA

http://www.csl.sri.com/index.shtml

Last Modified : Wednesday, 17-Dec-97 10:47:45 PST

SRI, International Computer Science Laboratory

webmaster@csl.sri.com

EXHIBIT
D

INTERNET ARCHIVE WaybackMachine

Enter Web Address: http:// All Take Me Back Adv. Search Compare Archive Pages

Searched for http://www.csl.sri.com/intrusion.html **33** Results

* denotes when site was updated.

Search Results for Jan 01, 1996 - Jul 24, 2006

1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006
0 pages	1 pages	2 pages	1 pages	3 pages	5 pages	9 pages	6 pages	5 pages	1 pages	0 pages
	Jul 05, 1997 *	Jan 24, 1998	Apr 28, 1999	Apr 09, 2000 *	Apr 07, 2001 *	Feb 08, 2002	Feb 11, 2003	Feb 02, 2004	Feb 06, 2005	
		Dec 05, 1998 *		Aug 15, 2000	Jun 19, 2001	Jun 03, 2002	Apr 12, 2003	Apr 03, 2004		
				Oct 26, 2000	Aug 16, 2001 *	Aug 11, 2002 *	Jun 05, 2003	Apr 04, 2004		
					Nov 12, 2001	Oct 03, 2002 *	Aug 10, 2003	Jun 07, 2004		
					Dec 01, 2001	Oct 12, 2002	Nov 28, 2003	Oct 10, 2004		
						Nov 11, 2002 *	Dec 03, 2003			
						Nov 25, 2002				
						Dec 02, 2002				
						Dec 09, 2002				

Home | Help

Internet Archive | Terms of Use | Privacy Policy

EXHIBIT
E

SRI International/Computer Science Laboratory

Intrusion Detection Home Page

EMERALD Page

NIDES Page

IDS Web Links

CSL Home Page

SRI Home Page

Research Opportunities!!

History of Intrusion Detection at SRI/CSL
Computer Science Laboratory, SRI International,
Menlo Park CA 94025-3493 USA

SRI International's Computer Science Laboratory (CSL) has been actively involved in intrusion-detection research since 1983. The original groundwork for SRI's intrusion-detection research explored statistical techniques for audit-trail reduction and analysis. The first-generation statistics component was used to analyze System Management Facility (SMF) records from an IBM mainframe system in the first half of the 1980s. Later, this research examined the use of a rule-based expert system to detect known malicious activity. This early research led to the development of a prototype Intrusion-Detection Expert System (IDES), capable of providing real-time detection of security violations on single-target host systems. IDES was a critical first step toward the development of real-time dual-analysis (signature analysis and anomaly-detection) intrusion-detection technology for monitoring security-critical government computing environment. By 1990, efforts began to integrate the IDES (later NIDES) prototype into a real-world computing environment (see the FBI FOIMS project).

With the maturity of the analysis methodologies developed under IDES, SRI began a comprehensive effort to enhance, optimize, and re-engineer the earlier IDES prototype into a production-quality intrusion-detection system called Next-Generation Intrusion Detection Expert System (NIDES). NIDES introduced a results-fusion component called the Resolver to integrate its response logic with the results produced by the statistical anomaly-detection subsystem and PBEST signature analysis tool. The NIDES statistical subsystem (NIDES/Stats) employs a wide range of multivariate statistical measures to profile the behavior of individual users or other computational entities. Analysis is profile-based, where a statistical score is assigned to each session representing how closely currently observed usage corresponds to the established patterns of usage for that individual. NIDES/Stats produces a separate usage profile for each user or other entity, and updates individual profiles as their corresponding audit records are encountered. NIDES also included a signature analysis component, developed using PBEST, to characterize known intrusive activity through rule encodings. Lastly, NIDES added an X/Motif-based graphical user interface facility to provide location-independent configuration and monitoring of NIDES operation and greatly increase usability.

The IDES/NIDES work pioneered the field of intrusion-detection, and sought to solve a difficult problem with a general and flexible approach, with no inherent restrictions on target systems, type of audit data to be analyzed, and techniques to be used. IDES/NIDES sought to address the need for user-oriented monitoring and profiling with a general and flexible approach, with no inherent restrictions on target systems, type of audit data to be analyzed, and techniques to be used. These efforts did, however, have some inherent limitations in scalability, applicability to network environments by their focus on users as the analysis targets, and lack of features to support interoperability. In addition, IDES/NIDES did not include features to address the more global threats from multi-domain coordinated attacks. CSL's Safeguard effort subsequently overcame profile explosion and scalability problems by profiling the activities of subsystems and commands rather than of individual users.

Current Research: *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances.*
Co-Principal Investigators: Phillip A. Porras (porras@csl.sri.com) and Peter G. Neumann

(neumann@csl.sri.com). In our current DARPA project (Contract F30602-96-C-0294, Analysis and Response for Intrusion Detection in Large Networks), we are developing a successor system to NIDES, EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances) that will considerably extend the NIDES concept to accommodate network-based analyses and dramatically increase interoperability and ease of integration into distributed computing environments. This effort will include extending components for profile-based analysis, signature-based analysis, and localized results fusion with automated response capability. In addition, we are considerably extending our results analysis capability to facilitate hierarchical interpretations of our distributed monitoring units, which will enable cross-platform analysis at various layers of abstraction, and successive refinement of the resulting analyses within increasingly broader scopes. We are also developing an accompanying set of exportable API that will permit interoperability between EMERALD components and network monitoring facilities.

Summary of Intrusion-Detection Research at SRI's Computer Science Laboratory:

- **Analysis and Response for Misuse Detection in Large Networks.** *[SRI Project 1494, Contract Number F30602-96-C-0294, DARPA ITO Order No. E302, 28 August 1996 through 27 August 1999].* Phillip Porras and Peter Neumann are leading a project to develop EMERALD (Event Monitoring Enabling Response to Anomalous Live Disturbances), a distributed scalable tool suite for tracking malicious activity through and across large networks. EMERALD introduces a highly distributed, building-block approach to network surveillance, attack isolation, and automated response. The approach is novel in its use of highly distributed, independently tunable, surveillance and response monitors that are deployable polymorphically at various abstract layers in a large network. These monitors demonstrate a streamlined intrusion-detection design that combines signature analysis with statistical profiling to provide localized real-time protection of the most widely used network services on the Internet. Equally important, EMERALD introduces a framework for coordinating the dissemination of analyses from the distributed monitors to provide a global detection and response capability to counter attacks occurring across an entire network enterprise. Also, EMERALD introduces a versatile application-programmers' interface that enhances its ability to integrate with the target hosts and provides a high degree of interoperability with third-party tool suites. See the EMERALD Home Page for details, postscript documents, and future availability of prototype releases.
- **Safeguard: Detecting Unusual Program Behavior Using the NIDES Statistical Component.** *[SRI Project 2596, Contract Number 910097C (Trusted Information Systems) under F30602-91-C-0067 (Rome Labs), 1995].* Debra Anderson led a project to adapt the NIDES statistical anomaly-detection subsystem to profile the behavior of individual applications. Statistical measures were customized to measure and differentiate the proper operation of an application from operation that may indicate Trojan horse substitution. Under the Safeguard model, analysis is application-based, where a statistical score is assigned to the operation of applications and represents the degree to which current behavior of the application corresponds to its established patterns of operation. The Safeguard effort demonstrated the ability of statistical profiling tools to clearly differentiate the scope of execution among general-purpose applications. It also showed that statistical analyses can be very effective in analyzing activities other than individual users; by instead monitoring applications, the Safeguard analysis greatly reduced the required number of profiles and computational requirements, and also decreased the typical false-positive and false-negative ratios. These results suggest the possible utility of performing statistical analyses on activities at higher layers of abstraction.
- **Next-Generation IDES (NIDES).** *[SRI Project 3131, Contract Number N00039-92-C-0015, 1992-1994].* Teresa Lunt and R. Jagannathan led an extensive effort to rearchitect and consolidate earlier IDES research results and prototypes into a production-quality tool suite. Most notably, NIDES

incorporated distributed audit collection and consolidation mechanisms to address the need for multi-host intrusion-detection coverage. It also provided significant enhancement to the statistical analysis algorithms and rule-based expert system, as well as introducing an X-Window GUI for administrative control and monitoring. In February 1993, CSL released the alpha-version of NIDES, and the final NIDES Beta2 Release was completed in September 1994 for Sun Microsystems SunOS 4.1.4 for Sun and SPARC workstations. See the NIDES Home Page for details, postscript documents, and availability of NIDES Software.

- **IDES for a Network of Workstations.** *[SRI Project 6784, Contract Number N00039-89-C-0050, ending 1992].* Teresa Lunt led a project to extend CSL's prototype Intrusion Detection Expert System (IDES) to be able to simultaneously monitor users on a network of Sun workstations and a DEC machine at SRI. The prototype IDES runs on several Sun 3 Workstations.
- **FOIMS-IDES, for the FBI Field Office Information System.** [SRI Project 6768, Contract J-FBI-88-171, 1991-93]. FOIMS is a classified IBM mainframe-based system used by FBI field offices throughout the U.S. to manage their cases. Following a previous one-year study that established the feasibility of applying IDES to the FOIMS environment, this contract implemented a version of IDES for FOIMS -- although it was not deployed in other than test environments. (Cleared insiders tend to be trusted, even if not trustworthy.)
- **The Enhanced IDES Prototype.** *[SRI Project 4185, Contract Number 9-X5H-4074J-1, Los Alamos National Laboratory, Government Prime Contarct No. W-7405-ENG-36, SPAWAR, ending 1988].* Teresa Lunt led a project to enhance CSL's prototype Intrusion Detection Expert System (IDES). The prototype IDES is based on the IDES model developed at SRI. The prototype IDES runs on a Sun 3 Workstation and is able to monitor, in real time, all users from an SRI target system, to adaptively learn user behavior patterns, and to detect abnormal behavior on the target system. This project also added an expert system component to IDES. Other enhancements included adding additional intrusion-detection measures, improving the statistical algorithms, monitoring more users and more event types, improving performance, and improving the user interface. Under this contract, SRI also performed a feasibility study for the FBI for implementing an IDES for their nationwide information system FOIMS.
- **Real-Time Intrusion Detection Expert System (IDES) Prototype.** *[SRI Project 7508-200, U.S. Government Contract N66001-84-D-0077, Delivery Order 0019, for the Space and Naval Warfare Command (SPAWAR), ending 1985].* SRI developed a prototype Intrusion Detection Expert System (IDES) to demonstrate proof-of-concept. The initial prototype ran on a SUN/3 workstation and could monitor, in real time, some users and some event types from an SRI target system, adaptively learn user behavior patterns, and detect some types of abnormal behavior on the target system. This project demonstrated that departures from normal user behavior can be detected in real-time.
- **Audit Trail Analysis and Usage Data Collection and Processing.** *[SRI Project 5910, Defense Communications Agency Contract DCA 200-83-C-0025, ending 1984].* Peter Neumann led the design and development of an audit-trail analyzer for TAC logins on MILNET/ARPANET, providing both live detection and after-the-intrusion analysis. This work was also applicable to the auditing of classified networks.
- **Intrusion Detection Expert System (IDES Model).** *[SRI Project 6169-70, Amendment 5 to U.S. Government Contract 83F83-01-00 for SPAWAR, 15 July 1984 to 16 September 1985].* Dorothy Denning and Peter Neumann developed a model for a real-time Intrusion-Detection System (IDES). This model forms the basis for the prototype IDES.
- **Statistical Techniques Development for an Audit Trail System.** *[SRI Project 6169, U.S. Government Contract 83F83-01-00, 15 July 1983 to 30 November 1986].* In this study, an extensive statistical analysis was performed on Government-furnished audit data from IBM systems running MVS and VM. A high-speed algorithm was developed that could accurately discriminate between users based on their behavior profiles. The project demonstrated that users can be distinguished from one another by their behavior profiles. These statistical procedures are potentially capable of

reducing the audit trail by a factor of 100 while demonstrating a high degree of accuracy in detecting intrusion attempts. Harold Javitz led the project, assisted by Dorothy Denning, Al Valdes, and Peter Neumann.

[Return to Top]

(*Last updated March 7, 1997. For more information please contact* intrusion@csl.sri.com)

SRI International/Computer Science Laboratory

Intrusion Detection Home Page

EMERALD Page

NIDES Page

IDS Web Links

CSL Home Page

SRI Home Page

[Click here for our latest publications on Intrusion Detection]

[1/19/98: Over 1,000 pages of newly released technical material on NIDES]

History of Intrusion Detection at SRI/CSL
Computer Science Laboratory, SRI International,
Menlo Park CA 94025-3493 USA

SRI International's Computer Science Laboratory (CSL) has been actively involved in intrusion-detection research since 1983. The original groundwork for SRI's intrusion-detection research explored statistical techniques for audit-trail reduction and analysis. The first-generation statistics component was used to analyze System Management Facility (SMF) records from an IBM mainframe system in the first half of the 1980s. Later, this research examined the use of a rule-based expert system to detect known malicious activity. This early research led to the development of a prototype Intrusion-Detection Expert System (IDES), capable of providing real-time detection of security violations on single-target host systems. IDES was a critical first step toward the development of real-time dual-analysis (signature analysis and anomaly-detection) intrusion-detection technology for monitoring security-critical government computing environment. By 1990, efforts began to integrate the IDES (later NIDES) prototype into a real-world computing environment (see the FBI FOIMS project).

With the maturity of the analysis methodologies developed under IDES, SRI began a comprehensive effort to enhance, optimize, and re-engineer the earlier IDES prototype into a production-quality intrusion-detection system called Next-Generation Intrusion Detection Expert System (NIDES). NIDES introduced a results-fusion component called the Resolver to integrate its response logic with the results produced by the statistical anomaly-detection subsystem and PBEST signature analysis tool. The NIDES statistical subsystem (NIDES/Stats) employs a wide range of multivariate statistical measures to profile the behavior of individual users or other computational entities. Analysis is profile-based, where a statistical score is assigned to each session representing how closely currently observed usage corresponds to the established patterns of usage for that individual. NIDES/Stats produces a separate usage profile for each user or other entity, and updates individual profiles as their corresponding audit records are encountered. NIDES also included a signature analysis component, developed using PBEST, to characterize known intrusive activity through rule encodings. Lastly, NIDES added an X/Motif-based graphical user interface facility to provide location-independent configuration and monitoring of NIDES operation and greatly increase usability.

The IDES/NIDES work pioneered the field of intrusion-detection, and sought to solve a difficult problem with a general and flexible approach, with no inherent restrictions on target systems, type of audit data to be analyzed, and techniques to be used. IDES/NIDES sought to address the need for user-oriented monitoring and profiling with a general and flexible approach, with no inherent restrictions on target systems, type of audit data to be analyzed, and techniques to be used. These efforts did, however, have some inherent limitations in scalability, applicability to network environments by their focus on users as the analysis targets, and lack of features to support interoperability. In addition, IDES/NIDES did not include features to address the more global threats from multi-domain coordinated attacks. CSL's Safeguard effort subsequently overcame profile explosion and scalability problems by profiling the

activities of subsystems and commands rather than of individual users.

Current Research: *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances.* Co-Principal Investigators: Phillip A. Porras (porras@csl.sri.com) and Peter G. Neumann (neumann@csl.sri.com). In our current DARPA project (Contract F30602-96-C-0294, Analysis and Response for Intrusion Detection in Large Networks), we are developing a successor system to NIDES, EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances) that will considerably extend the NIDES concept to accommodate network-based analyses and dramatically increase interoperability and ease of integration into distributed computing environments. This effort will include extending components for profile-based analysis, signature-based analysis, and localized results fusion with automated response capability. In addition, we are considerably extending our results analysis capability to facilitate hierarchical interpretations of our distributed monitoring units, which will enable cross-platform analysis at various layers of abstraction, and successive refinement of the resulting analyses within increasingly broader scopes. We are also developing an accompanying set of exportable API that will permit interoperability between EMERALD components and network monitoring facilities.

Summary of Intrusion-Detection Research at SRI's Computer Science Laboratory:

- **Analysis and Response for Misuse Detection in Large Networks.** *[SRI Project 1494, Contract Number F30602-96-C-0294, DARPA ITO Order No. E302, 28 August 1996 through 27 August 1999].* Phillip Porras and Peter Neumann are leading a project to develop EMERALD (Event Monitoring Enabling Response to Anomalous Live Disturbances), a distributed scalable tool suite for tracking malicious activity through and across large networks. EMERALD introduces a highly distributed, building-block approach to network surveillance, attack isolation, and automated response. The approach is novel in its use of highly distributed, independently tunable, surveillance and response monitors that are deployable polymorphically at various abstract layers in a large network. These monitors demonstrate a streamlined intrusion-detection design that combines signature analysis with statistical profiling to provide localized real-time protection of the most widely used network services on the Internet. Equally important, EMERALD introduces a framework for coordinating the dissemination of analyses from the distributed monitors to provide a global detection and response capability to counter attacks occurring across an entire network enterprise. Also, EMERALD introduces a versatile application-programmers' interface that enhances its ability to integrate with the target hosts and provides a high degree of interoperability with third-party tool suites. See the EMERALD Home Page for details, postscript documents, and future availability of prototype releases.
- **Safeguard: Detecting Unusual Program Behavior Using the NIDES Statistical Component.** *[SRI Project 2596, Contract Number 910097C (Trusted Information Systems) under F30602-91-C-0067 (Rome Labs), 1995].* Debra Anderson led a project to adapt the NIDES statistical anomaly-detection subsystem to profile the behavior of individual applications. Statistical measures were customized to measure and differentiate the proper operation of an application from operation that may indicate Trojan horse substitution. Under the Safeguard model, analysis is application-based, where a statistical score is assigned to the operation of applications and represents the degree to which current behavior of the application corresponds to its established patterns of operation. The Safeguard effort demonstrated the ability of statistical profiling tools to clearly differentiate the scope of execution among general-purpose applications. It also showed that statistical analyses can be very effective in analyzing activities other than individual users; by instead monitoring applications, the Safeguard analysis greatly reduced the required number of profiles and computational requirements, and also decreased the typical false-positive and false-negative ratios. These results suggest the possible utility of performing statistical analyses on activities at higher

layers of abstraction.

- **Next-Generation IDES (NIDES).** *[SRI Project 3131, Contract Number N00039-92-C-0015, 1992-1994].* Teresa Lunt and R. Jagannathan led an extensive effort to rearchitect and consolidate earlier IDES research results and prototypes into a production-quality tool suite. Most notably, NIDES incorporated distributed audit collection and consolidation mechanisms to address the need for multi-host intrusion-detection coverage. It also provided significant enhancement to the statistical analysis algorithms and rule-based expert system, as well as introducing an X-Window GUI for administrative control and monitoring. In February 1993, CSL released the alpha-version of NIDES, and the final NIDES Beta2 Release was completed in September 1994 for Sun Microsystems SunOS 4.1.4 for Sun and SPARC workstations. See the NIDES Home Page for details, postscript documents, and availability of NIDES Software.
- **IDES for a Network of Workstations.** *[SRI Project 6784, Contract Number N00039-89-C-0050, ending 1992].* Teresa Lunt led a project to extend CSL's prototype Intrusion Detection Expert System (IDES) to be able to simultaneously monitor users on a network of Sun workstations and a DEC machine at SRI. The prototype IDES runs on several Sun 3 Workstations.
- **FOIMS-IDES, for the FBI Field Office Information System.** [SRI Project 6768, Contract J-FBI-88-171, 1991-93]. FOIMS is a classified IBM mainframe-based system used by FBI field offices throughout the U.S. to manage their cases. Following a previous one-year study that established the feasibility of applying IDES to the FOIMS environment, this contract implemented a version of IDES for FOIMS -- although it was not deployed in other than test environments. (Cleared insiders tend to be trusted, even if not trustworthy.)
- **The Enhanced IDES Prototype.** *[SRI Project 4185, Contract Number 9-X5H-4074J-1, Los Alamos National Laboratory, Government Prime Contarct No. W-7405-ENG-36, SPAWAR, ending 1988].* Teresa Lunt led a project to enhance CSL's prototype Intrusion Detection Expert System (IDES). The prototype IDES is based on the IDES model developed at SRI. The prototype IDES runs on a Sun 3 Workstation and is able to monitor, in real time, all users from an SRI target system, to adaptively learn user behavior patterns, and to detect abnormal behavior on the target system. This project also added an expert system component to IDES. Other enhancements included adding additional intrusion-detection measures, improving the statistical algorithms, monitoring more users and more event types, improving performance, and improving the user interface. Under this contract, SRI also performed a feasibility study for the FBI for implementing an IDES for their nationwide information system FOIMS.
- **Real-Time Intrusion Detection Expert System (IDES) Prototype.** *[SRI Project 7508-200, U.S. Government Contract N66001-84-D-0077, Delivery Order 0019, for the Space and Naval Warfare Command (SPAWAR), ending 1985].* SRI developed a prototype Intrusion Detection Expert System (IDES) to demonstrate proof-of-concept. The initial prototype ran on a SUN/3 workstation and could monitor, in real time, some users and some event types from an SRI target system, adaptively learn user behavior patterns, and detect some types of abnormal behavior on the target system. This project demonstrated that departures from normal user behavior can be detected in real-time.
- **Audit Trail Analysis and Usage Data Collection and Processing.** *[SRI Project 5910, Defense Communications Agency Contract DCA 200-83-C-0025, ending 1984].* Peter Neumann led the design and development of an audit-trail analyzer for TAC logins on MILNET/ARPANET, providing both live detection and after-the-intrusion analysis. This work was also applicable to the auditing of classified networks.
- **Intrusion Detection Expert System (IDES Model).** *[SRI Project 6169-70, Amendment 5 to U.S. Government Contract 83F83-01-00 for SPAWAR, 15 July 1984 to 16 September 1985].* Dorothy Denning and Peter Neumann developed a model for a real-time Intrusion-Detection System (IDES). This model forms the basis for the prototype IDES.
- **Statistical Techniques Development for an Audit Trail System.** *[SRI Project 6169, U.S. Government Contract 83F83-01-00, 15 July 1983 to 30 November 1986].* In this study, an extensive

statistical analysis was performed on Government-furnished audit data from IBM systems running MVS and VM. A high-speed algorithm was developed that could accurately discriminate between users based on their behavior profiles. The project demonstrated that users can be distinguished from one another by their behavior profiles. These statistical procedures are potentially capable of reducing the audit trail by a factor of 100 while demonstrating a high degree of accuracy in detecting intrusion attempts. Harold Javitz led the project, assisted by Dorothy Denning, Al Valdes, and Peter Neumann.

[Return to Top]

(*Last updated March 7, 1997. For more information please contact* intrusion@csl.sri.com)

EXHIBIT
F

INTERNET ARCHIVE WaybackMachine

Enter Web Address: http:// All Take Me Back Adv. Search Compare Archive Pages

Searched for http://www.csl.sri.com/emerald/index.html

30 Results

* denotes when site was updated.

Search Results for Jan 01, 1996 - Jul 24, 2006

1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006
0 pages	1 pages	2 pages	3 pages	4 pages	5 pages	4 pages	6 pages	4 pages	1 pages	0 pages
	Jul 05, 1997 *	Jan 24, 1998 *	Feb 25, 1999 *	Apr 25, 2000 *	Apr 07, 2001 *	Aug 11, 2002 *	Feb 10, 2003	Feb 02, 2004 *	Feb 06, 2005	
		Dec 02, 1998 *	Apr 20, 1999	Jul 09, 2000 *	Jun 29, 2001 *	Nov 05, 2002 *	Jun 18, 2003	Feb 10, 2004 *		
			Apr 28, 1999 *	Aug 18, 2000	Jun 29, 2001 *	Nov 05, 2002 *	Jun 28, 2003 *	Apr 10, 2004		
				Oct 26, 2000	Nov 12, 2001	Dec 23, 2002 *	Aug 05, 2003 *	Jun 22, 2004		
					Dec 12, 2001		Oct 09, 2003 *			
							Dec 11, 2003 *			

Home | Help

Internet Archive | Terms of Use | Privacy Policy

EXHIBIT G

Event Monitoring Enabling Response To Anomalous Live Disturbances

Computer Science Laboratory

The EMERALD research team greatfully acknowledges funding support from the following agency:

Defense Advanced Research Projects Agency
Information Technology Office (ITO)
Contract No. F30602-96-C-0294

[6-19-1997]

(please address questions to emerald@csl.sri.com)

Event Monitoring Enabling Response To Anomalous Live Disturbances

Computer Science Laboratory

The EMERALD research team greatfully acknowledges funding support from the following agency:

Defense Advanced Research Projects Agency
Information Technology Office (ITO)
Contract No. F30602-96-C-0294

[6-19-1997]

(please address questions to emerald@csl.sri.com)

EXHIBIT
H

INTERNET ARCHIVE WaybackMachine

Enter Web Address: http:// All Take Me Back Adv. Search Compare Archive Pages

Searched for http://www.csl.sri.com/emerald/downloads.html

24 Results

* denotes when site was updated.

Search Results for Jan 01, 1996 - Jul 24, 2006

1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006
0 pages	0 pages	2 pages	0 pages	3 pages	5 pages	5 pages	4 pages	4 pages	1 pages	0 pages
		Jan 24, 1998 *		May 20, 2000 *	Mar 03, 2001 *	Jun 30, 2002 *	Jan 10, 2003	Feb 02, 2004	Feb 06, 2005	
		Dec 03, 1998 *		Aug 15, 2000	Apr 19, 2001 *	Oct 12, 2002 *	Feb 01, 2003	Apr 05, 2004		
				Aug 16, 2000 *	Jun 19, 2001	Oct 19, 2002	Oct 05, 2003	Jun 11, 2004		
					Aug 16, 2001 *	Nov 11, 2002 *	Dec 11, 2003	Oct 21, 2004		
					Dec 22, 2001	Nov 27, 2002				

Home | Help

Internet Archive | Terms of Use | Privacy Policy

EXHIBIT
I

The EMERALD Project

Current Downloads as of
(9/4/97)

January 5 1997	EMERALD: Conceptual Overview Statement (1.5 pgs)
Sept. 4 1997	• EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances (To appear in the 1997 National Information Systems Security Conference) (HTML) • EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances (To appear in the 1997 National Information Systems Security Conference) (Postcript)
Nov. 10 1997	• Live Traffic Analysis of TCP/IP Gateways (HTML) • Live Traffic Analysis of TCP/IP Gateways (To appear in the 1998 Internet Society Symposium on Network and Distributed System Security, March 1998) (Postscript)

EXHIBIT
J

To appear in the Internet Society's _Networks and Distributed Systems Security Symposium_, March 1998.

Live Traffic Analysis of TCP/IP Gateways

Phillip A. Porras
porras@csl.sri.com
Computer Science Laboratory

SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025

Alfonso Valdes
avaldes@csl.sri.com
Electromagnetic and Remote Sensing Laboratory
SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025

The work presented in this paper is currently funded by DARPA/ITO under contract number F30602-96-C-0294.

Point of Contact: Phillip A. Porras
Phone: (415) 859-3232
Fax: (415) 859-2844

November 10 1997

ABSTRACT

We enumerate a variety of ways to extend both statistical and signature-based intrusion-detection analysis techniques to monitor network traffic. Specifically, we present techniques to analyze TCP/IP packet streams that flow through network gateways for signs of malicious activity, nonmalicious failures, and other exceptional events. The intent is to demonstrate, by example, the utility of introducing gateway surveillance mechanisms to monitor network traffic. We present this discussion of gateway surveillance mechanisms as complementary to the filtering mechanisms of a large enterprise network, and illustrate the usefulness of surveillance in directly enhancing the security and stability of network operations.

---

1. Introduction

Mechanisms for parsing and filtering hostile external network traffic [2],[4] that could reach inter become widely accepted as prerequisites for limiting the exposure of internal network assets while r interconnectivity with external networks. The encoding of filtering rules for packet- or transport-la should be enforced at entry points between internal networks and external traffic. Developing filteri optimal balance between the restrictiveness necessary to suppress the entry of unwanted traffic, whi flows demanded for user functionality, can be a nontrivial exercise [3].

In addition to intelligent filtering, there have been various developments in recent years in passive s to monitor network traffic for signs of malicious or anomalous (e.g., potentially erroneous) activity. provide network administrators timely insight into noteworthy exceptional activity. Real-time moni dimension of control and insight into the flow of traffic between the internal network and its externa insight gained through fielded network traffic monitors could also aid sites in enhancing the effectiv filtering rules.

However, traffic monitoring is not a free activity--especially live traffic monitoring. In presenting o analysis techniques, we fully realize the costs they imply with respect to computational resources a example, obtaining the necessary input for surveillance involves the deployment of instrumentation format event streams derived from potentially high-volume packet transmissions. Complex event a and human management of the analysis units also introduce costs. Clearly, the introduction of netw mechanisms on top of already-deployed protective traffic filters is an expense that requires justificat outline the benefits of our techniques and seek to persuade the reader that the costs can be worthwhi

2. Toward Generalized Network Surveillance

The techniques presented in this paper are extensions of earlier work by SRI in developing analytica anomalous or known intrusive activity [1], [5], [12], [13]. Our earlier intrusion-detection efforts in c (Intrusion Detection Expert System) and later NIDES (Next-Generation Intrusion Detection Expert toward the surveillance of; user-session and host-layer activity. This previous focus on session acti boundaries is understandable given that the primary input to intrusion-detection tools, audit data, is that tend to be locally administered within a single host or domain. However, as the importance of r grown, so too has the need to expand intrusion-detection technology to address network infrastructu current research effort, EMERALD (Event Monitoring Enabling Responses to Anomalous Live Dis the extension of our intrusion-detection methods to the analysis of network activity.

Network monitoring, in the context of fault detection and diagnosis for computer network and telec environments, has been studied extensively by the network management and alarm correlation com [16]. The high-volume distributed event correlation technology promoted in some projects provides for building truly scalable network-aware surveillance technology for misuse. However, these effor health and status (fault detection and/or diagnosis) or performance of the target network, and do not intentionally abusive traffic. Indeed, some simplifications in the fault analysis and diagnosis comm of stateless correlation, which precludes event ordering; simplistic time-out metrics for resetting the

ignoring individuals/sources responsible for exceptional activity) do not translate well to a maliciou detecting intrusions.

Earlier work in the intrusion-detection community attempting to address the issue of network survei Network Security Monitor (NSM), developed at UC Davis [6], and the Network Anomaly Detectior (NADIR) [7], developed at Los Alamos National Laboratory (LANL). Both performed broadcast L analyze traffic patterns for known hostile or anomalous activity.[i] Further research by UC Davis ir Detection System (DIDS) [23] and later Graph-based Intrusion Detection System (GRIDS) [25] pro extend intrusion monitoring capabilities beyond LAN analysis, to provide multi-LAN and very larg

This paper takes a pragmatic look at the issue of packet and/or datagram analysis based on statistica signature-analysis techniques. This work is being performed in the context of SRI's latest intrusion- EMERALD, a distributed scalable tool suite for tracking malicious activity through and across large EMERALD introduces a building-block approach to network surveillance, attack isolation, and autc approach employs highly distributed, independently tunable, surveillance and response monitors tha polymorphically at various abstract layers in a large network. These monitors demonstrate a stream design that combines signature analysis with statistical profiling to provide localized real-time prote used network services and components on the Internet.

Among the general types of analysis targets that EMERALD monitors are network gateways. We d techniques that EMERALD implements, and discuss their use in analyzing malicious, faulty, and ot activity. EMERALD's surveillance modules will monitor entry points that separate external networ enterprise network and its constituent local domains.[ii] We present these surveillance techniques as filtering mechanisms of a large enterprise network, and illustrate their utility in directly enhancing t of network operations.

We first consider the candidate event streams that pass through network entry points. Critical to the operations is the careful selection and organization of these event streams such that an analysis base stream will provide meaningful insight into the target activity. We identify effective analytical tech event stream given specific analysis objectives. Sections 4 and 5 explore how both statistical anom signature analysis can be applied to identify activity worthy of review and possible response. All su by examples. More broadly, in Section 6 we discuss the correlation of analysis results produced by deployed independently throughout the entry points of our protected intranet. We discuss how even to a local surveillance monitor may be aggregated with results from other strategically deployed mo into more wide-scale problems or threats against the intranet. Section 7 discusses the issue of respo

3. Event Stream Selection

The success or failure of event analysis should be quantitatively measured for qualities such as accu both are assessable through testing. A more difficult but equally important metric to assess is compl network surveillance, inaccuracy is reflected in the number of legitimate transactions flagged as abn positives), incompleteness is reflected in the number of harmful transactions that escape detection (f performance is measured by the rate at which transactions can be processed. All three measurement directly depend on the quality of the event stream upon which the analysis is based. Here, we consic providing real-time surveillance of TCP/IP-based networks for malicious or exceptional network tra network surveillance mechanisms can be integrated onto, or interconnected with, network gateways a protected intranet and external networks.

IP traffic represents an interesting candidate event stream for analysis. Individually, packets represe records, where key data within the header and data segment can be statistically analyzed and/or heu response-worthy activity. However, the sheer volume of potential packets dictates careful assessme organize packets into streams for efficient parsing. Thorough filtering of events and event fields suc is concisely isolated, should be applied early in the processing stage to reduce resource utilization.

With respect to TCP/IP gateway traffic monitoring, we have investigated a variety of ways to categ of packets from an arbitrary packet stream. Individual packet streams can be filtered based on differ such as

- *Discarded traffic:* packets not allowed through the gateway because they violate filtering rule
- *Pass-through traffic:* packets allowed into the internal network from external sources.
- *Protocol-specific traffic:* packets pertaining to a common protocol as designated in the packet the stream of all ICMP packets that reach the gateway.
- *Unassigned port traffic:* packets targeting ports to which the administrator has not assigned a that also remain unblocked by the firewall.
- *Transport management messages:* packets involving transport-layer connection establishment (e.g., TCP SYN, RESET, ACK, `[window resize]`).
- *Source-address monitoring:* packets whose source addresses match well-known external sites satellite offices) or have raised suspicion from other monitoring efforts.
- *Destination-address monitoring:* all packets whose destination addresses match a given inter
- *Application-layer monitoring:* packets targeting a particular network service or application. T translate to parsing packet headers for IP/port matches (assuming an established binding betw rebuilding datagrams.

In the following sections we discuss how such traffic streams can be statistically and heuristically a into malicious and erroneous external traffic. Alternative sources of event data are also available fro produced by the various gateways, firewalls, routers, and proxy-servers (e.g., router syslogs can in f packet information from several products). We explore how statistical and signature analysis techni monitor various elements within TCP/IP event streams that flow through network gateways. We pre for detecting external entities that attempt to subvert or bypass internal network services. Technique detecting attacks against the underlying network infrastructure, including attacks using corruption o traffic in an attempt to negatively affect routing services, application-layer services, or other networ how to extend our surveillance techniques to recognize network faults and other exceptional activit of distributed result correlation.

4. Traffic Analysis with Statistical Anomaly Detection

SRI has been involved in statistical anomaly-detection research for over a decade [1], [5], [10]. Our on the profiling of user activity through audit-trail analysis. Within the EMERALD project, we are statistical algorithms to profile various aspects of network traffic in search of response- or alert-wor

The statistical subsystem tracks subject activity via one or more variables called *measures*. The stati four classes of measures: categorical, continuous, intensity, and event distribution. *Categorical* mea assume values from a categorical set, such as originating host identity, destination host, and port nu measures are those for which observed values are numeric or ordinal, such as number of bytes trans also track the intensity of activity (that is, the rate of events per unit time) and the ``meta-distributio

affected by recent events. These derived measure types are referred to as *intensity* and *event distribu*

The system we have developed maintains and updates a description of a subject's behavior with resp types in a compact, efficiently updated *profile*. The profile is subdivided into short- and long-term e profile accumulates values between updates, and exponentially ages values for comparison to the lo: consequence of the aging mechanism, the short-term profile characterizes the recent activity of the s determined by the dynamically configurable aging parameters used. At update time (typically, a tim the update function folds the short-term values observed since the last update into the long-term pro profile is cleared. The long-term profile is itself slowly aged to adapt to changes in subject activity. compares related attributes in the short-term profile against the long-term profile. As all evaluations empirical distributions, no assumptions of parametric distributions are made, and multi-modal and c are accommodated. Furthermore, the algorithms we have developed require no *a priori* knowledge c exceptional activity. A more detailed mathematical description of these algorithms is given in [9], [2

Our earlier work considered the subject class of users of a computer system and the corresponding e audit trail generated by user activity. Within the EMERALD project, we generalize these concepts s software such as network gateways, proxies, and network services can themselves be made subject c event streams are obtained from log files, packet analysis, and--where required--special-purpose ins services of interest (e.g., FTP, HTTP, or SMTP). As appropriate, an event stream may be analyzed a multiple subjects, and the same network activity can be analyzed in several ways. For example, an e packets permits analyses that track the reason each packet was rejected. Under such a scenario, the f packet is the subject, and the measures of interest are the reason the packet was dropped (a categoric of dropped packets in the recent past (one or more intensity measures tuned to time intervals of secc Alternatively, these dropped packets may be parsed in finer detail, supporting other analyses where example, the identity of the originating host.

EMERALD can also choose to separately define satellite offices and ``rest of world" as different sul stream. That is, we expect distinctions from the satellite office's use of services and access to assets sessions originating from external nonaffiliated sites. Through satellite session profiling, EMERALI signs of unusual activity. In the case of the FTP service, for example, each user who gives a login na ``anonymous" is a subject as well. Another example of a subject is the network gateway itself, in wh subject. All subjects for the same event stream (that is, all subjects within a subject class) have the s their profiles, but the internal profile values are different.

As we migrate our statistical algorithms that had previously focused on user audit trails with users a our ability to build more abstract profiles for varied types of activity captured within our generalizec stream. In the context of statistically analyzing TCP/IP traffic streams, profiling can be derived fron perspectives, including profiles of

- Protocol-specific transactions (e.g., all ICMP exchanges)
- Sessions between specific internal hosts and/or specific external sites
- Application-layer-specific sessions (e.g., anonymous FTP sessions profiled individually and/c
- Discarded traffic, measuring attributes such as volume and disposition of rejections
- Connection requests, errors, and unfiltered transmission rates and disposition

Event records are generated either as a result of activity or at periodic intervals. In our case, activity content of IP packets or transport-layer datagrams. Our event filters also construct interval summary accumulated network traffic statistics (at a minimum, number of packets and number of kilobytes tr: are constructed at the end of each interval (e.g., once per N seconds).

EMERALD's statistical algorithm adjusts its short-term profile for the measure values observed on t distribution of recently observed values is evaluated against the long-term profile, and a distance be obtained. The difference is compared to a historically adaptive, subject-specific deviation. The empi deviation is transformed to obtain a score for the event. Anomalous events are those whose scores e adaptive, subject-specific score threshold based on the empirical score distribution. This nonparame measure types and makes no assumptions on the modality of the distribution for continuous measur

The following sections provide example scenarios of exceptional network activity that can be meas statistical engine deployed to network gateways.

4.1 Categorical Measures in Network Traffic

Categorical measures assume values from a discrete, nonordered set of possibilities. Examples of ca include

- Source/destination address: One expects, for example, accesses from satellite offices to origin host identities.
- Command issued: While any single command may not in itself be anomalous, some intrusion ``doorknob rattling") give rise to an unusual mix of commands in the short-term profile.
- Protocol: As with commands, a single request of a given protocol may not be anomalous, but protocol requests, reflected in the short-term profile, may indicate an intrusion.
- Errors and privilege violations: We track the return code from a command as a categorical me distribution to reflect only a small percent of abnormal returns (the actual rate is learned in th While some rate of errors is normal, a high number of exceptions in the recent past is abnorm in unusual frequencies for abnormal categories, detected here, and unusual count of abnormal continuous measure as described in Section 4.2.
- Malformed service requests: Categorical measures can track the occurrence of various forms malformed packets directed to a specific network service.
- Malformed packet disposition: Packets are dropped by a packet filter for a variety of reasons, innocuous (for example, badly formed packet header). Unusual patterns of packet rejection or lead to insight into problems in neighboring systems or more serious attempts by external site
- File handles: Certain subjects (for example, anonymous FTP users) are restricted as to which Attempts to access other files or to write read-only files appear anomalous Such events are of signature analysis as well.

The statistical component builds empirical distributions of the category values encountered, even if is open-ended, and has mechanisms for ``aging out" categories whose long-term probabilities drop b

The following is an example of categorical measures used in the surveillance of proxies for services Consider a typical data-exchange sequence between an external client and an internal server within Anonymous FTP is restricted to certain files and directories; the names of these are categories for m file/directory reads and (if permitted) writes. Attempted accesses to unusual directories appear anon dedicated to ports include a categorical measure whose values are the protocol used. Invalid request violation error; the type of error associated with a request is another example of a categorical measu of errors in the recent past is tracked as continuous measures, as described in Section

4.2 Continuous Measures in Network Traffic

Continuous measures assume values from a continuous or ordinal set. Examples include inter-event stamps between consecutive events from the same stream), counting measures such as the number o type observed in the recent past, and network traffic measures (number of packets and number of ki subsystem treats continuous measures by first allocating bins appropriate to the range of values of tl and then tracking the frequency of observation of each value range. In this way, multi-modal distrib and much of the computational machinery used for categorical measures is shared.

Continuous measures are useful not only for intrusion detection, but also support the monitoring of l network from the perspective of connectivity and throughput. An instantaneous measure of traffic v gateway monitor can detect a sudden and unexpected loss in the data rate of received packets, when historical norms for the gateway. This sudden drop is specific both to the gateway (the subject, in th of day (e.g., the average sustained traffic rate for a major network artery is much different at 11:00 a

In our example discussion of an FTP service in Section 4.1, attempts to access unallowed directorie The recently observed rate of such errors is continuously compared with the rate observed over simi FTP sessions. Some low rate of error due to misspellings or innocent attempts is to be expected, and in the historical profile for these measures. An excess beyond historical norms indicates anomalous

Continuous measures can also work in conjunction with categorical measures to detect excessive da uploads, or excessive mail relaying, as well as excessive service-layer errors by external clients. Cat measures have proven to be the most useful for anomaly detection in a variety of contexts.

We next describe the two derived measure types, *intensity* and *event distribution*, which detect anon traffic volume and the mix of measures affected by this traffic.

4.3 Measuring Network Traffic Intensity

Intensity measures distinguish whether a given volume of traffic appears consistent with historical c measures reflect the intensity of the event stream (number of events per unit time) over time interva Typically, we have defined three intensity measures per profile, which, with respect to user activity at intervals of 60 seconds, 600 seconds, and 1 hour. Applied to raw event streams, intensity measure for detecting flooding attacks, while also providing insight into other anomalies.

EMERALD uses volume analyses to help detect the introduction of malicious traffic, such as traffic denials or perform intelligence gathering, where such traffic may not necessarily be violating filterin increase in the overall volume of discarded packets, as well as analysis of the disposition of the disc discussed in Section 4.1, can provide insight into unintentionally malformed packets resulting from internal errors in neighboring hosts. High volumes of discarded packets can also indicate more mali transmissions such as scanning of UPD ports or IP address scanning via ICMP echoes. Excessive nu requests (EXPN) may indicate intelligence gathering, perhaps by spammers. These and other applicat doorknob rattling can be detected by an EMERALD statistical engine when filtering is not desired.

Alternatively, a sharp increase in events viewed across longer durations may provide insight into a c or prevent successful traffic flow. Intensity measures of transport-layer connection requests, such as SYN-RST messages, could indicate the occurrence of a SYN-attack [17] against port availability (o scanning). Variants of this could include intensity measures of TCP/FIN messages [14], considered port scanning.

Monitoring overall traffic volume and bursty events by using both intensity and continuous measure interesting advantages over other monitoring approaches, such as user-definable heuristic rules that In particular, the intensity of events over a duration is relative in the sense that the term ``high volur considered different at midnight than at 11:00 a.m. The notion of high bursts of events might similai of the target system in the intranet (e.g., web server host versus a user workstation). Rule developers define thresholds based on many factors unique to the target system. On the other hand, the statistic: time, build a target-specific profile that could evaluate event intensity for the given system over a vá as the time of day (e.g., business hours versus afterhours) and/or day of the week (e.g., weekday ver

4.4 Event Distribution Measures

The event-distribution measure is a meta-measure that monitors which other measures in the profile event. For example, an *ls* command in an FTP session affects the directory measure, but does not af: file transfer. This measure is not interesting for all event streams. For example, all network-traffic e' same measures (number of packets and kilobytes) defined for that event stream, so the event distribi

On the other hand, event-distribution measures are useful in correlative analysis achieved via the ``I approach. Here, each monitor contributes to an aggregate event stream for the domain of the correla events are generated only when the individual monitor decides that the recent behavior is anomalou: sufficiently anomalous by itself to trigger a declaration). Measures recorded include time stamp, mo identifier, and measure identities of the most outlying measures. Overall intensity of this event strea correlated attack. The distribution of which monitors and which measures are anomalous is likely to intrusion or malfunction than with the normal ``innocent exception." (See Section 6 for a further dis correlation.)

4.5 Statistical Session Analysis

Statistical anomaly detection via the methods described above enables EMERALD to answer questi current anonymous FTP session compares to the historical profile of all previous anonymous FTP s‹ could be similarly monitored for atypical exchanges (e.g., excessive mail relays).

Continuing with the example of FTP, we assign FTP-related events to a subject (the login user or ``ε sessions may be interleaved, we maintain separate short-term profiles for each, but may score again: profile (for example, short-term profiles are maintained for each ``anonymous" FTP session, but eac historical profile of ``anonymous" FTP sessions). The aging mechanism in the statistics module allo either as the events occur or at the end of the session. We have chosen the former approach (analyze as it potentially detects anomalous activity in a session before that session is concluded.

5. Traffic Analyzing with Signature Analysis

Signature analysis is a process whereby an event stream is mapped against abstract representations ‹ to indicate the target activity of interest. Signature engines are essentially expert systems whose rule are parsed that appear to indicate suspicious, if not illegal, activity. Signature rules may recognize si themselves represent significant danger to the system, or they may be chained together to recognize represent an entire penetration scenario.

However, simplistic event-to-rule binding alone does not necessarily provide enough indication to e of the target activity. Signature analyses must also distinguish whether an event sequence being witı transitioning the system into the anticipated compromised state. In addition, determining whether a ; indicative of an attack may be a function of the preconditions under which the event sequence is per schemes for representing operating system penetrations through audit trail analysis are [12], [18], [1

Using basic signature-analysis concepts, EMERALD can support a variety of analyses involving pa datagrams as event streams. For example, address spoofing, tunneling, source routing [21], SATAN and abuse of ICMP messages (`Redirect` and `Destination` Unreachable} messages in particular) [4 and detected by signature engines that guard network gateways. The heuristics for analyzing header datagrams for some of these abuses are not far from what is already captured by some filtering tools difficult to justify the expense of passively monitoring the traffic stream for such activity when one knowledge into filtering rules.[iv]

Regardless, there still remain several examples that help justify the expense of employing signature network traffic. In particular, there are points where the appearance of certain types of legitimate tra regarding the motives of the traffic source. Distinguishing benign requests from illicit ones may be questions are ultimately site-specific. For example, EMERALD surveillance modules can encode th activity such as the number of fingers, pings, or failed login requests to accounts such as guest, dem FTP, or employees who have departed the company. Threshold analysis is a rudimentary, inexpensi the occurrence of specific events and, as the name implies, detects when the number of occurrences reasonable count.

In addition, we are developing heuristics to support the processing of application-layer transactions monitoring. EMERALD's signature analysis module can sweep the data portion of packets in search transactions that indicate suspicious, if not malicious, intentions by the external client. While traffic external traffic through to an internally available network service, signature analysis offers an abilit transaction requests or request parameters, alone or in combination, that are indicative of attempts t abuse the internal service. EMERALD's signature engine, for example, is capable of real-time parsi the firewall or router for unwanted transfers of configuration or specific system data, or anonymous public portions of the directory structure. Similarly, EMERALD can analyze anonymous FTP sessic retrievals and uploads/modifications are limited to specific directories. Additionally, EMERALD's s capability is being extended to session analyses of complex and dangerous, but highly useful, servic

Another interesting application of signature analysis is the scanning of traffic directed at high-numb ports to which the administrator has not assigned a network service). Here, datagram parsing can be traffic after some threshold volume of traffic, directed at an unused port, has been exceeded. A sign a knowledge base of known telltale datagrams that are indicative of well-known network-service pr Telnet, SMTP, HTTP). The signature module then determines whether the unknown port traffic mat datagram sets. Such comparisons could lead to the discovery of network services that have been ins administrator's knowledge.

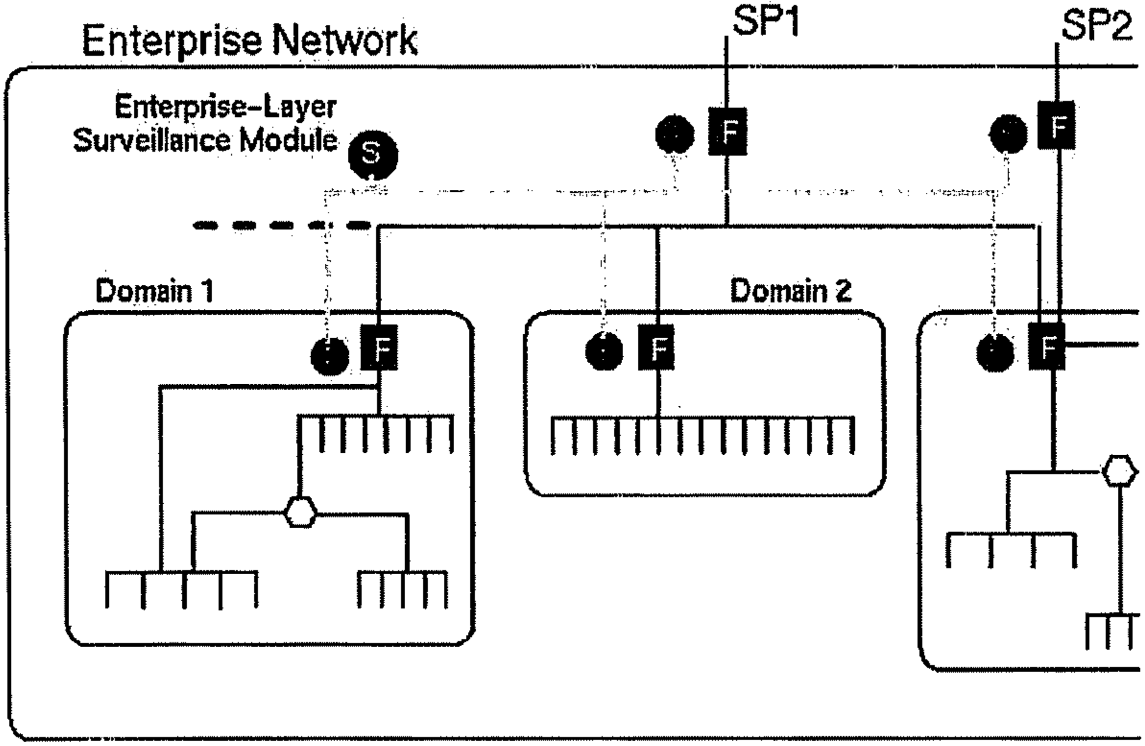
6. Composable Surveillance of Network Traffic

The focus of surveillance need not be limited to the analysis of traffic streams through a single gate extension of anomaly detection and signature analyses is to support the hierarchical correlation of a by multiple distributed gateway surveillance modules. Within the EMERALD framework, we are de

surveillance modules that analyze the anomaly and signature reports produced by individual traffic ı various entry points of external traffic into local network domains.

This concept is illustrated in Figure 1, which depicts an example enterprise network consisting of in network domains.[v] These local domains are independently administered, and could perhaps corres computing assets among departments within commercial organizations or independent laboratories ' organizations. In this figure, connectivity with the external world is provided through one or more s SP2), which may provide a limited degree of filtering based on source address (to avoid address spo primitive checks such as monitoring checksum.

Example Network Deployment of Surveillance Monitors



Inside the perimeter of the enterprise, each local domain maintains its traffic filtering control (F-box subnetworks. These filters enforce domain-specific restriction over issues such as UDP port availab: acceptable protocol traffic. EMERALD surveillance monitors are represented by the S-circles, and a various entry points of the enterprise and domains.

EMERALD surveillance modules develop analysis results that are then directed up to an enterprise- correlates the distributed results into a meta-event stream. The enterprise monitor is identical to the

monitors (i.e., they use the same code base), except that it is configured to correlate activity reports monitors. The enterprise monitor employs both statistical anomaly detection and signature analyses results produced by the distributed gateway surveillance modules, searching for commonalities or tr analysis results.

The following sections focus on aggregate analyses that may induce both local response and/or ente enumerate some of the possible ways that analysis results from the various surveillance modules car insight into more global problems not visible from the narrow perspective of local entry-point monit

6.1 Commonalities among Results

One issue of direct interest is whether there exist commonalities in analysis results across surveillan examining mutually exclusive event streams. For example, a scenario previously discussed was that observing a drastic increase in the number of discarded packets at the entry point to a domain, perha majority cause for packet discards. Depending on the degree of increase, a local domain administrat take actions to help alleviate or remove the cause of the failed packets. However, if on a given day a throughout the enterprise similarly observed marked increases in discarded packet volume, the respo from being a local concern to being an enterprise-wide issue. Similarly, commonalities across doma protocol-specific errors or signature engines detecting unwanted activity across multiple domains cc layer responses.

We might also choose to distinguish excessive types of certain traffic in an effort to check for intelli outsiders who submit requests such as finger, echo, or mail alias expansion, to multiple domains in t robin doorknob rattling). The objective of such a technique might be to avoid detection from both lc and/or continuous measures by spreading out the probes to multiple independently monitored domai analysis, we could maintain the enterprise-wide profile of probes of this type, and detect when an ur these probes occurs. While such probes may not appear excessive from the local domain perspective may observe a marked increase worthy of response.

In addition, we can add a layer of traffic-rate monitoring by profiling the overall volume of enterpris throughout various slices of the day and week. Local monitors may use continuous measures to dete packet volumes that could indicate transmission loss or serious degradation. However, it is conceiva from the local domain perspective, while significant, is not drastic enough to warrant active respons may find through results correlation that the aggregate of all domains producing reports of transmiss during the same time period could warrant attention at the enterprise layer. Thus, local domain activ warranting a response could in aggregation with other activity be found to warrant a response.

6.2 Sequential Trend Analysis

Of general use to meta-surveillance is the modeling of activity for sequential trends in the appearanc For example, this could entail correlating the analyses of local monitors, looking for trends in the pr layer datagrams for error or ICMP packets. While local responses to error messages could be handle administrators, reports of errors spreading across all domains might more effectively be addressed b connections between the enterprise and the service provider.

Attacks repeated against the same network service across multiple domains can also be detected thr

correlation. For example, multiple surveillance modules deployed to various local domains in the en report, in series, suspicious activity observed within sessions employing the same network service. S enterprise-layer responses or warnings to other domains that have not yet experienced or reported th this sense, results correlation enables the detection of spreading attacks against a common service, v one domain, and gradually spread domain by domain to affect operations across the enterprise.

We are studying the use of fault-relationship models [22], in which recognition of a problem in one (e.g., loss of connectivity or responsiveness) could propagate as different problems in neighboring h overflows or connection timeout due to overloads). Our enterprise monitor employs rule-based heur relationship models.

7. Response Handling

Once a problem is detected, the next challenge is to formulate an effective response. In many situati response may be no response at all, in that every response imposes some cost in system performanc The extent to which a decision unit contains logic to filter out uninteresting analysis results may me effective monitoring units and unmanageable (soon to be disabled) monitoring units. For certain ana detection of known hostile activity through signature analyses, the necessity for response invocation other analysis results such as anomaly reports, response units may require greater sophistication in t

Fundamental to effective response handling is the accurate identification of the source responsible f unlike audit-trail analysis where event-record fields such as the subject ID are produced by the OS k direct control over the content and format of packet streams. Packet forgery is straightforward, and avoid allowing attackers to manipulate response logic to harm legitimate user connectivity or cause throughout the network. Some techniques have been proposed to help track network activity to the s

Another issue is how to tailor a response that is appropriate given the severity of the problem, and th effect to address the problem without harming the flow of legitimate network traffic. Countermeasu passive responses, such as passive results dissemination, to highly aggressive actions, such as severi channel. Within EMERALD, our response capabilities will employ the following general forms of r

- **Passive results dissemination:** EMERALD monitors can make their analysis results availabl review. We are currently exploring techniques to facilitate passive dissemination of analysis r existing network protocols such as SNMP, including the translation of analysis results into an management information base (MIB) structure. However, whereas it is extremely useful to int dissemination into an already-existing infrastructure, we must balance this utility with the nee and integrity of analysis results.
- **Assertive results dissemination:** Analysis results can be actively disseminated as administra automatic dissemination of alerts may help to provide timely review of problems by administr be the most expensive form of response, in that it requires human oversight.[vi]
- **Dynamic controls over logging configuration:** EMERALD monitors can perform limited co configuration of logging facilities within network components (e.g., routers, firewalls, networ daemons).
- **Integrity checking probes:** EMERALD monitors may invoke handlers that validate the integ or other assets. Integrity probes may be particularly useful for ensuring that privileged networ subverted.[vii]
- **Reverse probing:** EMERALD monitors may invoke probes in an attempt to gather as much c

the source of suspicious traffic by using features such as *traceroute* or *finger*. However, care i
such actions, as discussed in [4].

- **Active channel termination:** An EMERALD monitor can actively terminate a channel sessi
known hostile activity. This is perhaps the most severe response, and care must be taken to en
manipulate the surveillance monitor to deny legitimate access.

8. Conclusion

We have described event-analysis techniques developed in the intrusion-detection community, and
application to monitoring TCP/IP packet streams through network gateways. We present a variety o
(both malicious and nonmalicious) to which these analysis techniques could be applied. Table 1 sun
exceptional network activity presented in this paper, and identifies which method (statistical anomal
analysis, or hierarchical correlation) can be utilized to detect the activity.

These examples help to justify the expense of gateway surveillance monitors, even in the presence c
filtering mechanisms. Indeed, several of the example forms of ``interesting traffic'' listed in Table 1
preventable using filtering mechanisms. In addition, our surveillance modules may even help to tun
filtering rules that could lead to the accidental discarding of legitimate traffic. The surveillance mod
occurrence of traffic that appears to be anomalous or abusive, regardless of whether the traffic is all
prevented from entering, through the network gateway. Furthermore, these techniques may extend t
detection such as failures in neighboring systems.

While this paper is intended to justify and illustrate the complementary nature of combining surveill
filtering mechanisms, in future research we will explore the practical aspects of monitor deploymen
analysis and secure integration into supporting network infrastructure (e.g., network management). I
traditional audit-based intrusion-detection developers, network monitor developers must carefully a
to organize and isolate the relevant traffic from which their analyses are based. The added dimensio
into network operations gained by well-integrated surveillance modules is well worth consideration.

Analysis Description	Stat. Categ. Meas.	Stat. Conti. Meas.	Stat. Inten. Meas.
Protocol-specific anomalies such as excessive data transfers (FTP uploads, mail relays, other huge data transfers)	X	X	X
Port/service misuse, including excessive errors or unknown command exchanges	X		X
Discarded packet volume			X
Discarded packet disposition (analysis of rejection patterns)	X	X	
Excessive transport-layer connection requests, including heavy syn-ack message usage	X		X
Anonymous session comparisons against historical usage	X	X	X
Satellite office profiling	X	X	X

Sudden drops or floods in data rate (specific to system, time of day, day of week, and so forth)		X	X
Address/port scanning and other general doorknob rattling			X
Excessive drops in line quality compared to historical quality		X	X
Detection of filterable events (e.g., ICMP message abuse, address spoofing, tunneling, source/port routing, SATAN signatures)			
Event thresholds for events reflecting site-specific concerns			
Detection of user-installed network services on unregistered ports			
Packet data sweeps for application-layer proxies, looking for troublesome data transfers or requests			
Aggregate analysis across the enterprise for round-robin doorknob rattling that attempts to defeat domain-layer intensity measures			
Aggregate analysis of low-level degradation of services or throughput across the enterprise			
Trend analysis for error propagation occurring across multiple domains			
Spreading attacks that may indicate worm or fault interrelationships among network modules			

Endnotes

i. Recent product examples, such as ASIM and Net Ranger, that follow the passive packet moni since gained wide deployment in some Department of Defense network facilities.
ii. We use the terms *enterprise* and *intranet* interchangeably; both exist ultimately as cooperative independently administered domains, communicating together with supportive network infras firewalls, routers, and bridges.
iii. Of particular added value in assessing this traffic would be some indication of why a given pa generic solution for deriving this *disposition* information without dependencies on the firewal Such information would be a useful enhancement to packet-rejection handlers.
iv. On the other hand, one may also suggest a certain utility in simply having real-time mechanis hierarchically correlate attempts by external sources to forward undesirable packets through a
v. This is one example network filtering strategy that is useful for illustrating result correlation. possible.
vi. Consider a network environment that on average supports 100,000 external transactions (the c analysis-target-specific) per day. Even if only 0.1% of the transactions were found worthy of administrators would be asked to review 100 transactions a day.
vii. A significant number of network attacks target the subversion of privileged network service. 97.16, CA-97.12, CA-97.05 give a few recent examples.

References

1. D.Anderson, T.Frivold, and A.Valdes. Next-generation intrusion-detection expert system (NI report. *Technical report,* Computer Science Laboratory, SRI International, Menlo Park, CA, 1

2. B.Chapman and E.Zwicky. *Building internet firewalls*. O'Reilly and Associates, Inc. Sebastop

3. D.Chapman. Network (in)security through IP packet filtering. In *Proceedings of the Third US Symposium*, Baltimore, MD, September 1992.

4. W.R. Cheswick and S.M. Bellovin. *Firewalls and internet security: Repelling the wily hacker* Reading, MA, 1994.

5. D.E. Denning. An intrusion-detection model. *IEEE Transactions on Software Engineering*, 1:

6. L.T. Heberlein, G.Dias, K.N. Levitt, B.Mukherjee, J.Wood, and D.Wolber. A network securit *Proceedings of the 1990 Symposium on Research in Security and Privacy*, pages 296-303, Oa IEEE Computer Society.

7. K.Jackson, D.DuBois, and C.Stallings. An expert system application for network intrusion de *of the Fourteenth Computer Security Group Conference*. Department of Energy, 1991.

8. G.Jakobson and M.D. Weissman. Alarm correlation. *IEEE Network*, pages 52-59, November

9. H.S. Javitz and A.Valdes. The NIDES statistical component description and justification. Tec Science Laboratory, SRI International, Menlo Park, CA, March 1994.

10. H.S. Javitz, A.Valdes, D.E. Denning, and P.G. Neumann. Analytical techniques development detection system (SIDS) based on accounting records. *Technical report,* SRI International, M 1986.

11. S.Kliger, S.Yemini, Y.Yemini, D.Ohsie, and S.Stolfo. A coding approach to event correlation *Fourth International Symposium on Integrated Network Management (IFIP/IEEE)*, Santa Bar 277. Chapman and Hall, London, England, May 1995.

12. T.F. Lunt, R.Jagannathan, R.Lee, A.Whitehurst, and S.Listgarten. Knowledge-based intrusion *Proceedings of the 1989 AI Systems in Government Conference*, March 1989.

13. T.F. Lunt, A.Tamaru, F.Gilham, R.Jagannathan, C.Jalali, P.G. Neumann, H.S. Javitz, and A.\ intrusion-detection expert system (IDES). *Technical report*, Computer Science Laboratory, SI Park, CA, 28 February 1992.

14. Uriel Maimon. Port scanning without the SYN flag. *Phrack Magazine*, vol. 7, issue 49.

15. M.Mansouri-Samani and M.Sloman. Monitoring distributed systems. *IEEE Network*, pages 2(

16. K.Meyer, M.Erlinger, J.Betser, C.Sunshine, G.Goldszmidt, and Y.Yemini. Decentralizing cor network management. In *Proceedings of the Fourth International Symposium on Integrated N (IFIP/IEEE)*, Santa Barbara, CA, pages 4-16. Chapman and Hall, London, England, May 199

17. RobertT. Morris. A weakness in the 4.2BSD UNIX TCP/IP software. In *Computing Science 1* AT&T Bell Laboratories, Murray Hills, NJ, 25 February 1985.

18. A.Mounji, B.Le Charlier, and D.Zampunieris. Distributed audit trail analysis. In *Proceedings Symposium on Network and Distributed System Security*, pages 102-112, February 1995.

19. P.A. Porras. STAT: A State Transition Analysis Tool for intrusion detection. Master's thesis, ‹
Department, University of California, Santa Barbara, July 1992.

20. P.A. Porras and P.G. Neumann. EMERALD: Event monitoring enabling responses to anomal‹
National Information Systems Security Conference, pages 353-365, Baltimore, MD, October

21. J.Postel. Internet protocol, request for comment, RFC 791. *Technical report,* Information Scie
1981.

22. L.Ricciulli and N.Shacham. Modeling correlated alarms in network management systems. In ‹
Networks and Distributed Systems Modeling and Simulation, 1997.

23. S.R. Snapp, J.Brentano, G.V. Dias, T.L Goan, L.T. Heberlein, C.-L. Ho, K.N. Levitt, B.Mukh
T.Grance, D.M. Teal, and D.Mansur. DIDS (Distributed Intrusion Detection System)--motiva
early prototype. In *Proceedings of the Fourteenth National Computer Security Conference*, pa
Washington, D.C., 1-4 October 1991. NIST/NCSC.

24. S.Staniford-Chen, S.Cheung, R.Crawford, M.Dilger, J.Frank, J.Hoagland, K.Levitt, C.Wee, R
GrIDS--a graph based intrusion detection system for large networks. In *Proceedings of the Ni
Information Systems Security Conference*, pages 361-370 (Volume I), Washington. D.C., Oct‹

25. S.Staniford-Chen and L.T. Heberlein. Holding intruders accountable on the internet. In *Proce
Symposium on Security and Privacy*, 1995.

26. A.Valdes and D.Anderson. Statistical methods for computer usage anomaly detection using N
the Third International Workshop on Rough Sets and Soft Computing (RSSC 94), San Jose, Ja

27. W.Venema. Project SATAN: UNIX/internet security. In *Proceedings of the COMPSEC-95 C
London, 1995.

EXHIBIT
K

INTERNET ARCHIVE

Enter Web Address: http:// All Take Me Back Adv. Search

Not in Archive.

The page you requested has not been archived. If the page is still available on the Internet, we will begin archiving it during our next crawl. Try another request or click here to search for all pages on http://ftp:/ftp.csl.sri.com/pub/gateway98.ps
See the FAQs for more info and help, or contact us.

Home | Help

Internet Archive | Terms of Use | Privacy Policy

EXHIBIT
L

Advanced Search

find this **URL** http://

between these **dates** (optional) Month Day Year
Month Day Year

Go Wayback

Other Advanced Search Options

URL Matching	◉	Retrieve page that most closely matches search criteria
	○	List all pages that match search criteria
Aliases	◉	Merge aliases (search results for yahoo.com, www.yahoo.com and yahoo.com/index.html will be merged together)
	○	Show aliases separately (a search for yahoo.com will list www.yahoo.com separately)
	○	Don't show aliases (a search for yahoo.com will not show www.yahoo.com)
Redirects	◉	Hide redirects (on the search results, we will not display pages that redirect to other pages)
	○	Flag redirects (on the search results, we will mark all pages that redirect to another page with an 'r')
	○	Show redirects (on the search results, we will display pages that redirect)
File Types	All types	Will only display files of the type you specify
Duplicates	☐	Show duplicates (if we have 20 identical versions of a page on the same day, we will show them all)
Comparison	☐	Show checkboxes to allow comparison of 2 versions of a page. Comparison technology provided by Docucomp.
Convert to PDF	☐	**(BETA)** Provide links to a service that will convert a version of a web page to PDF format. Conversion technology provided by 2Convert.

Advanced URL locator hints and tips

There are a number of easy URL-based queries for conducting Advanced Searches on the documents in the Wayback Machine. To conduct these Advanced Searches, simply enter the following URLs in your browser's location or address bar.

Retrieving the most recently archived copy of a specific URL

http://web.archive.org/http://www.cnet.com

where "http://www.cnet.com" is the target URL. This query returns the most recently archived version of that target URL in the archive.

Retrieving an archived copy of a specific URL from given date

http://web.archive.org/20011007203917/http://www.cnet.com

This returns a specific document whose URL matches the target URL and whose archive date most closely matches the date specified in the format YYYYMMDDhhmmss. In the example above, this returns www.cnet.com archived on October 7, 2001 at 8:39pm and 17 seconds.

The date need not be specified to the second. Using a truncated date will return an archived page that most closely matches the average value of the date specified.

Example of truncating to the Year
http://web.archive.org/2000/http://www.cnet.com

This returns the document whose URL exactly matches http://www.cnet.com and whose archival date most closely matches July 1, 2000 (July 1 is the middle of the year or the "average value" of the year 2000).

Example of truncating to the Year and Month
http://web.archive.org/200010/http://www.cnet.com

This returns the document whose URL exactly matches http://www.cnet.com and whose archival date most closely matches October 15, 2000 (the 15th is the middle of October or the "average value" of October, 2000).

Searching for all copies of a specific URL archived in a given time period

http://web.archive.org/200109*/http://www.cnet.com

This returns all copies of a specific target URL (e.g. http://www.cnet.com) which were archived beginning with the date specified in the format YYYYMMDDhhmmss. In the example above, this returns a list of all all archived versions of www.cnet.com archived in September 2001.

Searching for all URLs for a site archived in a given time period

http://web.archive.org/200109*/http://www.cnet.com*

This returns all URLs that begin with http://www.cnet.com which were archived in September 2001.

EXHIBIT
M

INTERNET ARCHIVE
WaybackMachine

Enter Web Address: http:// All Take Me Back Adv. Search

Searched for all pages on http://www.csl.sri.com/emerald Results **1** - **1** of about **1**

www.csl.sri.com/emerald/index.html
1 page from Jul 05, 1997

Results **1** - **1** of about **1** Previous 1 Next Results per page 10

Home | Help

Internet Archive | Terms of Use | Privacy Policy

EXHIBIT
N

INTERNET ARCHIVE
WaybackMachine

Enter Web Address: http:// All Take Me Back Adv. Search

Searched for all pages on http://www.csl.sri.com/emerald Results **1** - **10** of about **45**

www.csl.sri.com/emerald/
1 page from Jan 24, 1998

www.csl.sri.com/emerald/charts.html
1 page from Jan 24, 1998

www.csl.sri.com/emerald/concepts.html
1 page from Jan 24, 1998

www.csl.sri.com/emerald/downloads-intmain.html
1 page from Jan 24, 1998

www.csl.sri.com/emerald/downloads.html
1 page from Jan 24, 1998

www.csl.sri.com/emerald/emerald-niss97.html
1 page from Jan 24, 1998

www.csl.sri.com/emerald/emerald.html
1 page from Jan 24, 1998

www.csl.sri.com/emerald/index.html
1 page from Jan 24, 1998

www.csl.sri.com/emerald/links.html
1 page from Jan 24, 1998

www.csl.sri.com/emerald/live-traffic.html
1 page from Jan 24, 1998

Results **1** - **10** of about **45** Previous 1 2 3 4 5 **Next** Results per page 10

Home | Help

Internet Archive | Terms of Use | Privacy Policy

INTERNET ARCHIVE
WaybackMachine

Enter Web Address: http:// All Take Me Back Adv. Search

Searched for all pages on http://www.csl.sri.com/emerald Results **11** - **20** of about **45**

www.csl.sri.com/emerald/presentations/NISSC97/index.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/sld001.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/sld002.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/sld003.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/sld004.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/sld005.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/sld006.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/sld007.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/sld008.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/sld009.htm
1 page from Jan 24, 1998

Results **11** - **20** of about **45** **Previous** 1 2 3 4 5 **Next** Results per page 10

Home | Help

Internet Archive | Terms of Use | Privacy Policy

INTERNET ARCHIVE WaybackMachine

Enter Web Address: http:// All Take Me Back Adv. Search

Searched for all pages on http://www.csl.sri.com/emerald Results **21** - **30** of about **45**

www.csl.sri.com/emerald/presentations/NISSC97/sld010.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/sld011.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/sld012.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/sld014.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/sld015.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/sld016.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/tsld001.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/tsld002.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/tsld003.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/tsld004.htm
1 page from Jan 24, 1998

Results **21** - **30** of about **45** **Previous** 1 2 3 4 5 **Next** Results per page 10

Home | Help

Internet Archive | Terms of Use | Privacy Policy

INTERNET ARCHIVE
WaybackMachine

Enter Web Address: http:// All Take Me Back Adv. Search

Searched for all pages on http://www.csl.sri.com/emerald Results **31** - **40** of about **45**

www.csl.sri.com/emerald/presentations/NISSC97/tsld005.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/tsld006.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/tsld007.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/tsld008.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/tsld009.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/tsld010.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/tsld011.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/tsld012.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/tsld013.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/tsld014.htm
1 page from Jan 24, 1998

Results **31** - **40** of about **45** Previous 1 2 3 4 5 Next Results per page 10

INTERNET ARCHIVE WaybackMachine

Enter Web Address: http:// All Take Me Back Adv. Search

Searched for all pages on http://www.csl.sri.com/emerald Results **41** - **45** of about **45**

www.csl.sri.com/emerald/presentations/NISSC97/tsld015.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/presentations/NISSC97/tsld016.htm
1 page from Jan 24, 1998

www.csl.sri.com/emerald/project.html
1 page from Jan 24, 1998

www.csl.sri.com/emerald/sponsor.html
1 page from Jan 24, 1998

www.csl.sri.com/emerald/traffic-short.html
1 page from Jan 24, 1998

Results **41** - **45** of about **45** **Previous** 1 2 3 4 5 Next Results per page 10

Home | Help

Internet Archive | Terms of Use | Privacy Policy

EXHIBIT
O

Live Traffic Analysis of TCP/IP Gateways

Phillip A. Porras
porras@csl.sri.com
Computer Science Laboratory

SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025

Alfonso Valdes
avaldes@csl.sri.com
Electromagnetic and Remote Sensing Laboratory
SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025

The work presented in this paper is currently funded by DARPA/ITO under contract number F30602-96-C-0294.

Point of Contact: Phillip A. Porras
Phone: (415) 859-3232
Fax: (415) 859-2844

August 1 1997

ABSTRACT

We enumerate a variety of ways to extend both statistical and signature-based intrusion-detection analysis techniques to monitor network traffic. Specifically, we present techniques to analyze TCP/IP packet streams that flow through network gateways for signs of malicious activity, nonmalicious failures, and other exceptional events. The intent is to justify, by example, the expense (in computational resources and human oversight) of introducing network

surveillance mechanisms to monitor network traffic. We present this discussion of gateway surveillance modules as complementary to the filtering mechanisms of a large enterprise network, and illustrate their utility in directly enhancing the security and stability of network operations.

1. Introduction

Significant progress has been made toward the development of mechanisms to parse and filter hostile external network traffic, and thus prevent it from entering internal network environments [Firewalls94,Chapman95]. Mechanisms for preventing such traffic from reaching internal network services have become widely accepted as prerequisites for limiting the exposure of internal network assets, while providing interconnectivity with external networks. The encoding of filtering rules for packet or transport-layer communication should be enforced at key entry points between internal networks and external traffic. Developing filtering rules that strike an optimal balance between the restrictiveness necessary to suppress the entry of unwanted traffic, while allowing the necessary flows demanded for user functionality, can be a nontrivial exercise.

In addition to intelligent filtering, there have also been various developments in recent years in passive surveillance mechanisms to monitor network traffic for signs of malicious or anomalous (e.g., potentially erroneous) activity. Such tools attempt to provide network administrators timely insight into noteworthy exceptional activity. Realtime monitoring promises an added dimension of control and insight into the flow of traffic between the internal network and its external environment. The insight gained through fielded network traffic monitors could also aid sites in enhancing the effectiveness of their firewall filtering rules.

However, traffic monitoring is not a free activity---especially live traffic monitoring. Our discussion of network analysis techniques are presented fully realizing the costs they imply with respect to computational resources and human oversight. For example, obtaining the necessary input for surveillance involves the deployment of instrumentation to parse, filter, and format, event streams derived from potentially high-volume packet transmissions. Complex event analysis, response, and management of the units also introduce cost. Clearly, the introduction of network surveillance components on top of already deployed protective traffic filters is an expense that requires justification. In this paper, we outline the benefits of our techniques and seek to persuade the reader that these costs can be worthwhile.

[This paper will appear in the Proceedings of the
1998 Symposium on Network and Distributed System Security.
A final version will appear on this web page by November 1997.
Please check back then if you would like a copy. Thank you]